A Physical Unclonable Function based on Capacitor Mismatch in a Charge-Redistribution SAR-ADC

Qianying Tang, Won Ho Choi, Luke Everson, Keshab K. Parhi and Chris H. Kim

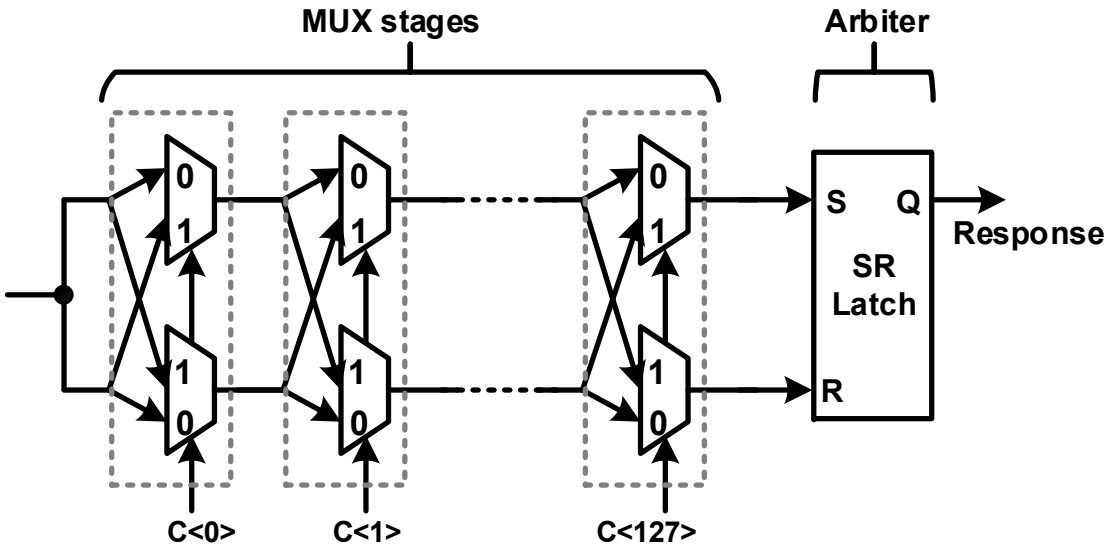
University of Minnesota
Department of Electrical and Computer Engineering
Minneapolis, MN 55455

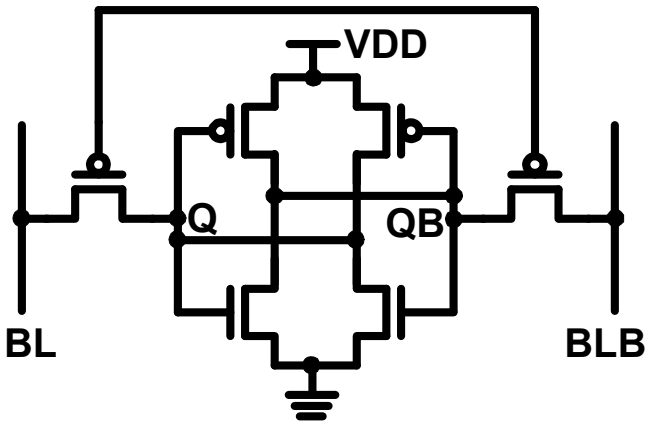
Outline

- Background and Motivation
- Proposed SAR-ADC PUF
- 65nm PUF Chip Data
- Summary

SAR-ADC: Successive Approximation Register Analog-to-Digital Converter
PUF: Physical Unclonable Function

Conventional PUFs

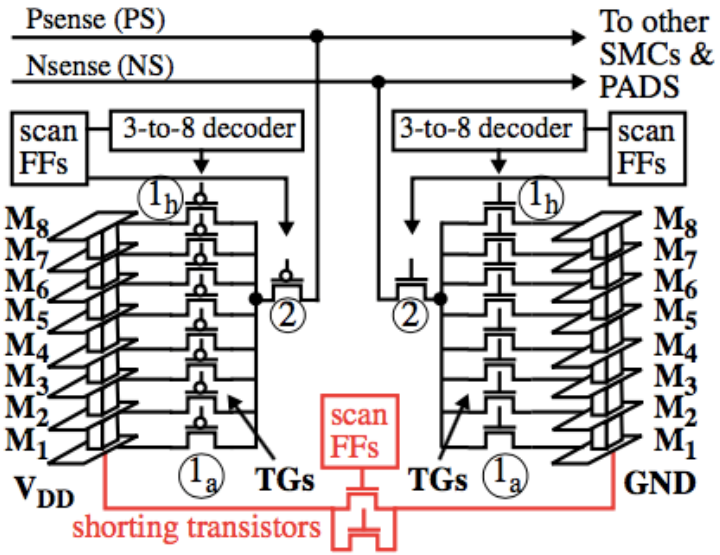




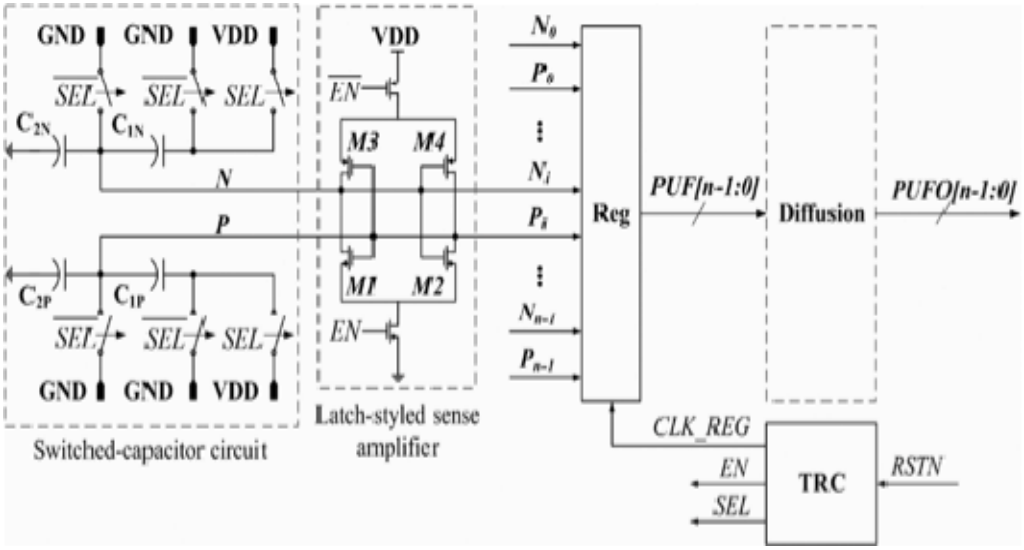
- **Arbiter PUF**:
  - Entropy source: Delay path variation
  - Number of challenge-response pairs (CRPs) exponentially proportional to the number of cells → strong PUF

- **SRAM PUF:**
  - Entropy source: Cell mismatch
  - Number of CRPs proportional to the number of cells → weak PUF

Passive Device based PUFs



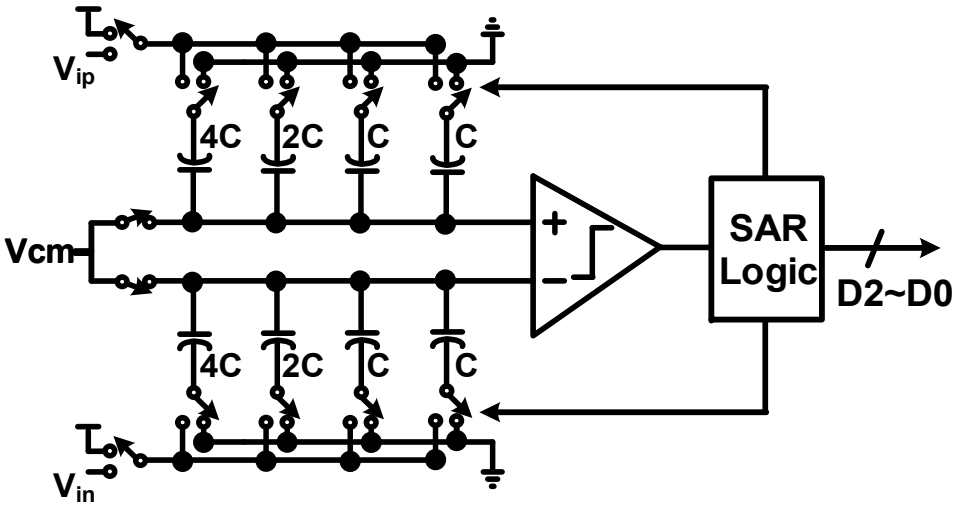
J. Ju, HOST, 2013

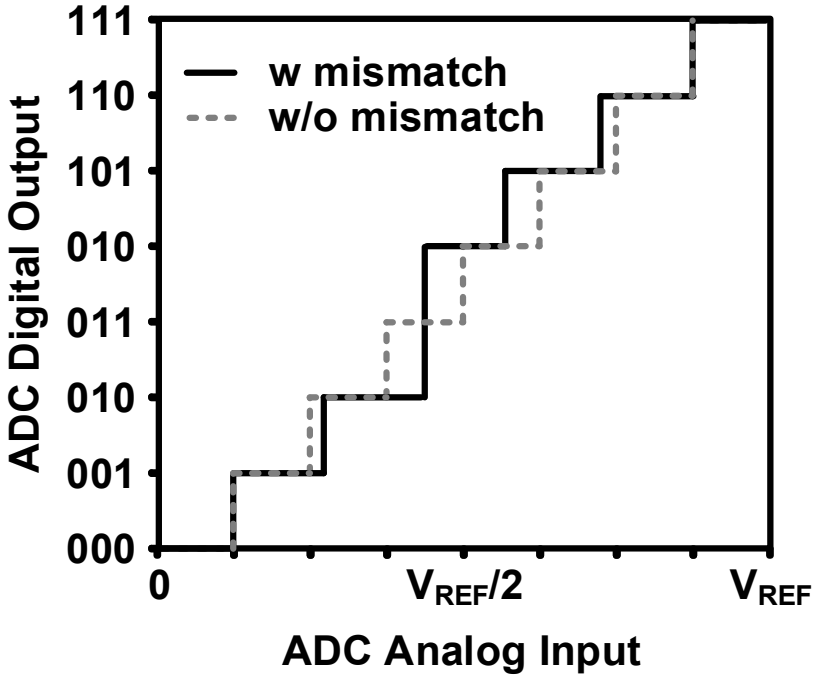


M. Wan, TCAS-I, 2015

- Passive devices are more stable under V, T variation as compared to active devices
  - Metal wire resistance variation in chip power grid (left)
  - Capacitance variation in switch capacitor circuit (right)

Contributions of This Work



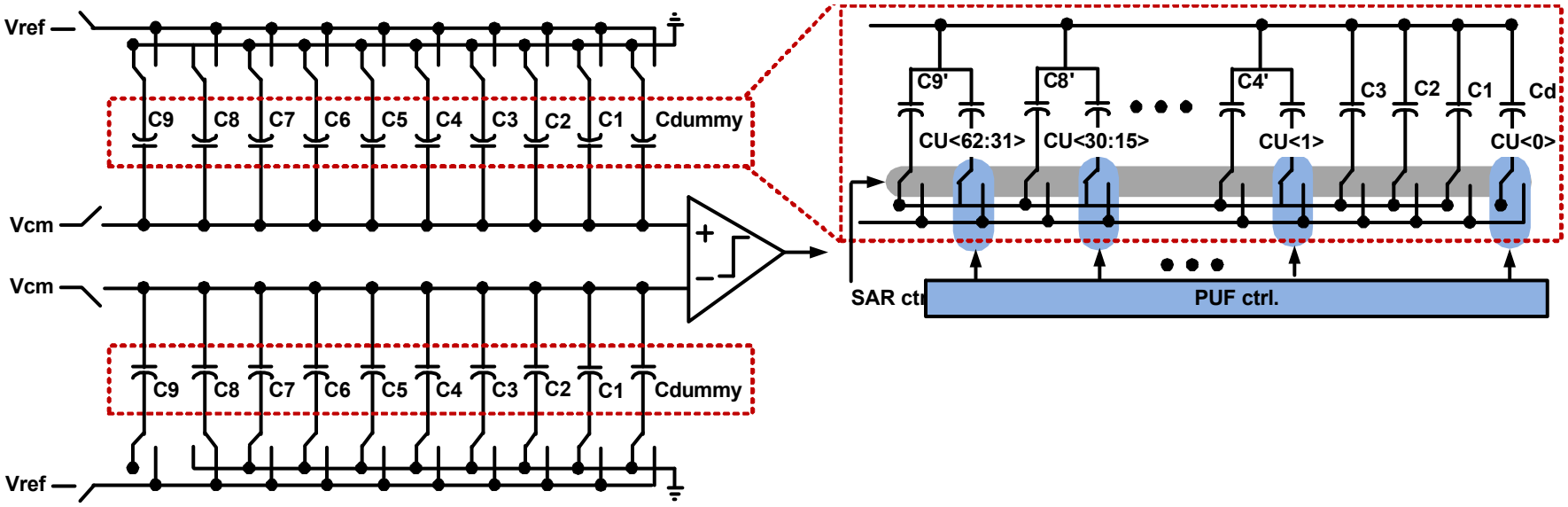


- Extract mismatch in capacitor array of standard charge redistribution SAR-ADC → minimal design and area overhead
- Experimentally verify if indeed passive PUFs are stable under V and T variations (so far, results are inconclusive)

Outline

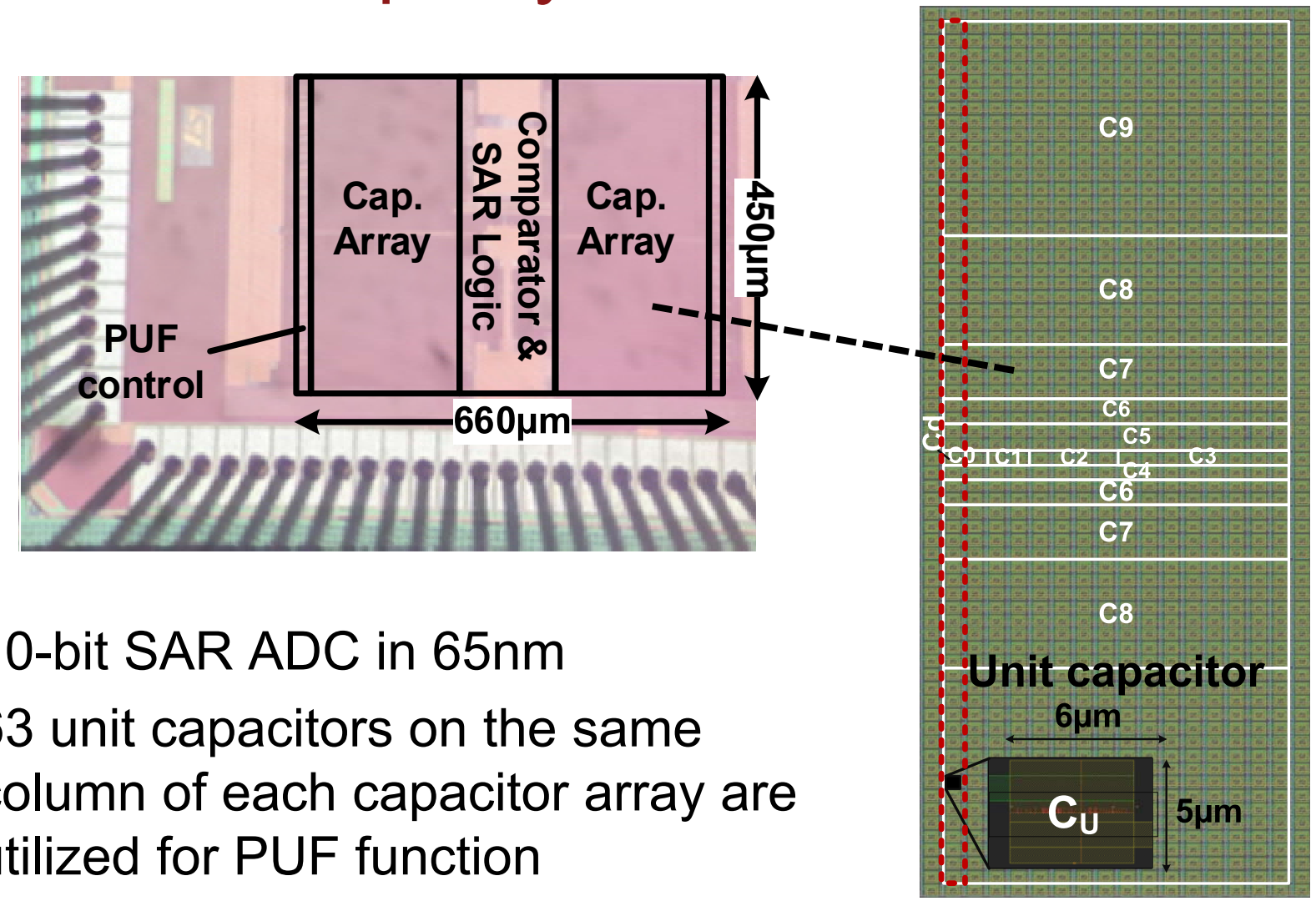
- Background and Motivation
- Proposed SAR-ADC PUF
- 65nm PUF Chip Data
- Summary

Modifications to Standard SAR-ADC



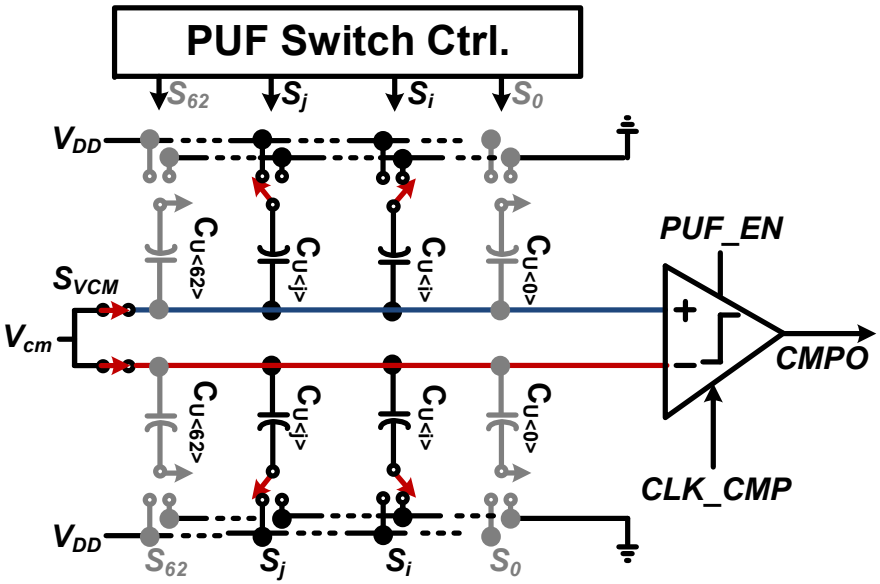
- 4% area overhead
  - PUF control logic
  - Independent control of unit caps
  - A counter to determine soft response (not shown here)

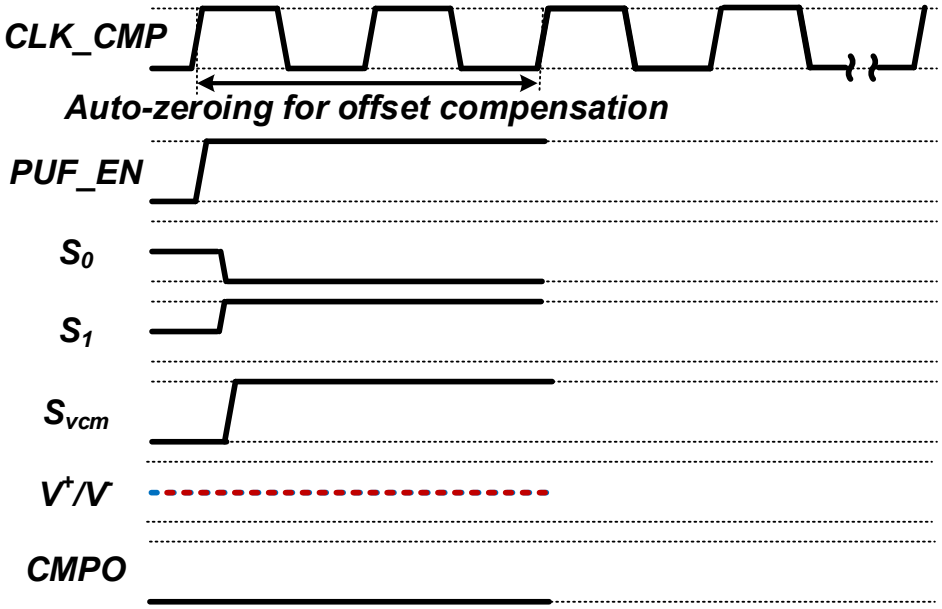
Test Chip Layout and Die Photo



- 10-bit SAR ADC in 65nm
- 63 unit capacitors on the same column of each capacitor array are utilized for PUF function

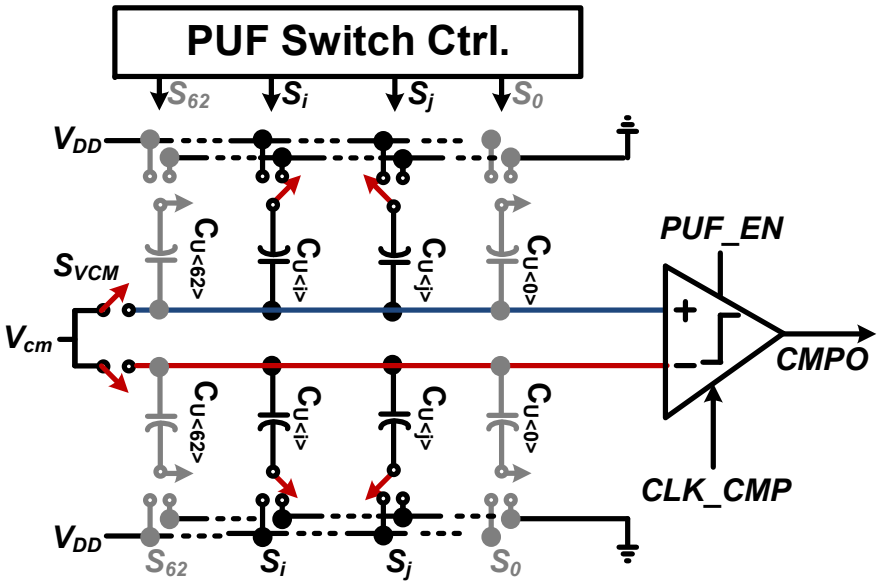
Step 1: Sampling Phase

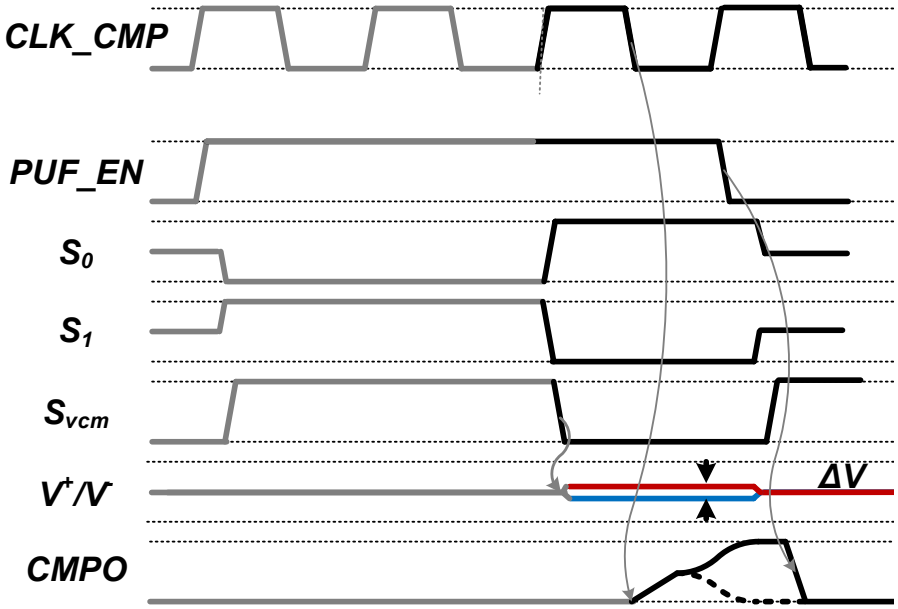




- V+ and V- are initialized to the common-mode voltage Vcm
  - Two unit capacitors are enabled and connected in series between VDD and GND
  - Charge on top plate: $Q = V_{cm} \cdot C_{U<i>} + \left(V_{cm} - V_{DD}\right) \cdot C_{U<j>}$

Step 2: Evaluation Phase

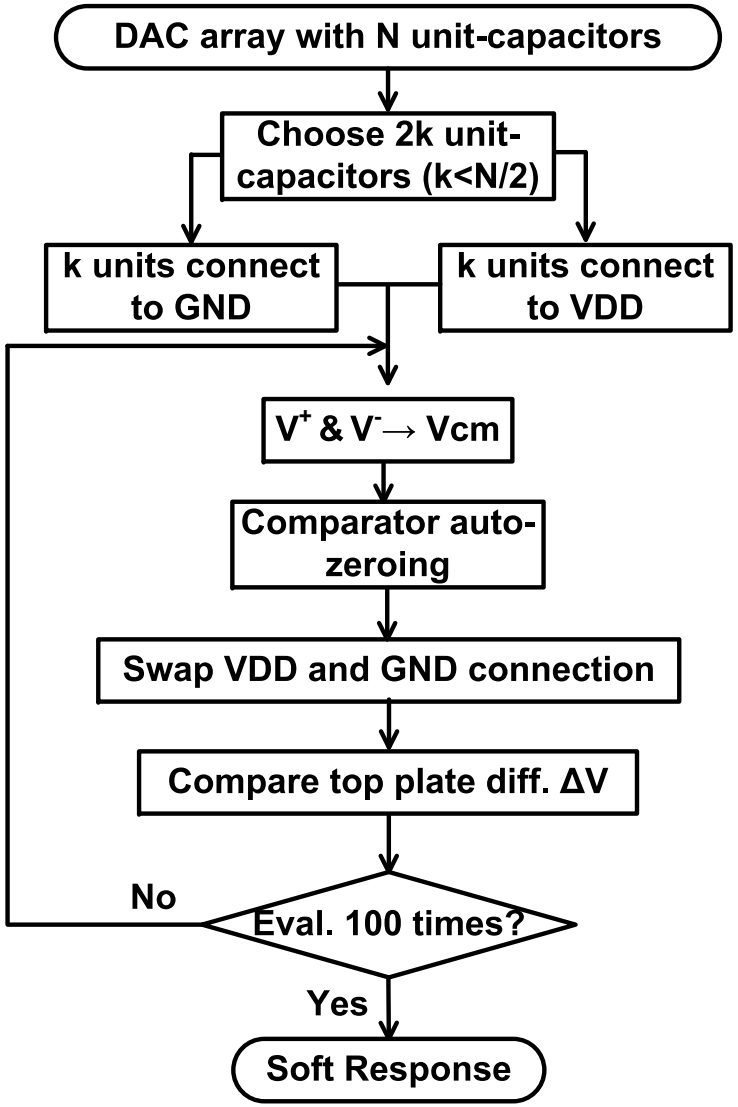


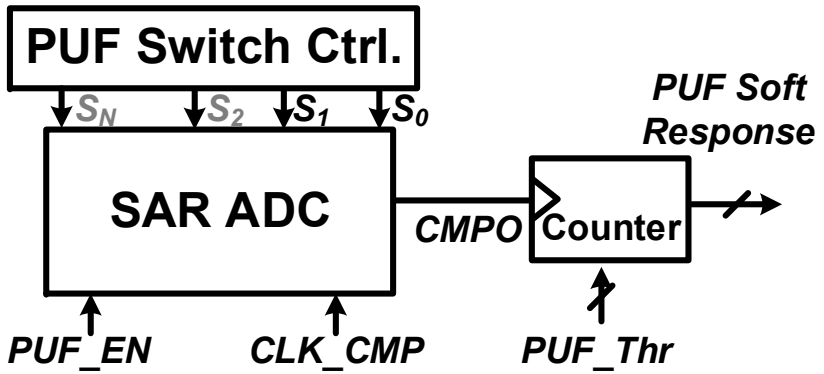


- Connection of S_i and S_j are swapped, Vcm is disconnected
  - Charge on top plate: $Q^+_{clk1} = Q^+_{clk3} \Rightarrow V^+ = V_{CM} - \frac{C^+_{U<i>} - C^+_{U<j>}}{C^+_{U<i>} + C^+_{U<j>}} V_{DD}$
  - Capacitance difference between $C_{U<i>}$ and $C_{U<j>}$ results in different input voltage ΔV:

$$\Delta V = V^+ - V^- = \left(\frac{C^-_{U<i>} - C^-_{U<j>}}{C^-_{U<i>} + C^-_{U<j>}} - \frac{C^+_{U<i>} - C^+_{U<j>}}{C^+_{U<i>} + C^+_{U<j>}} \right) \cdot V_{DD}$$

Overall Flow and Soft Response Measurement



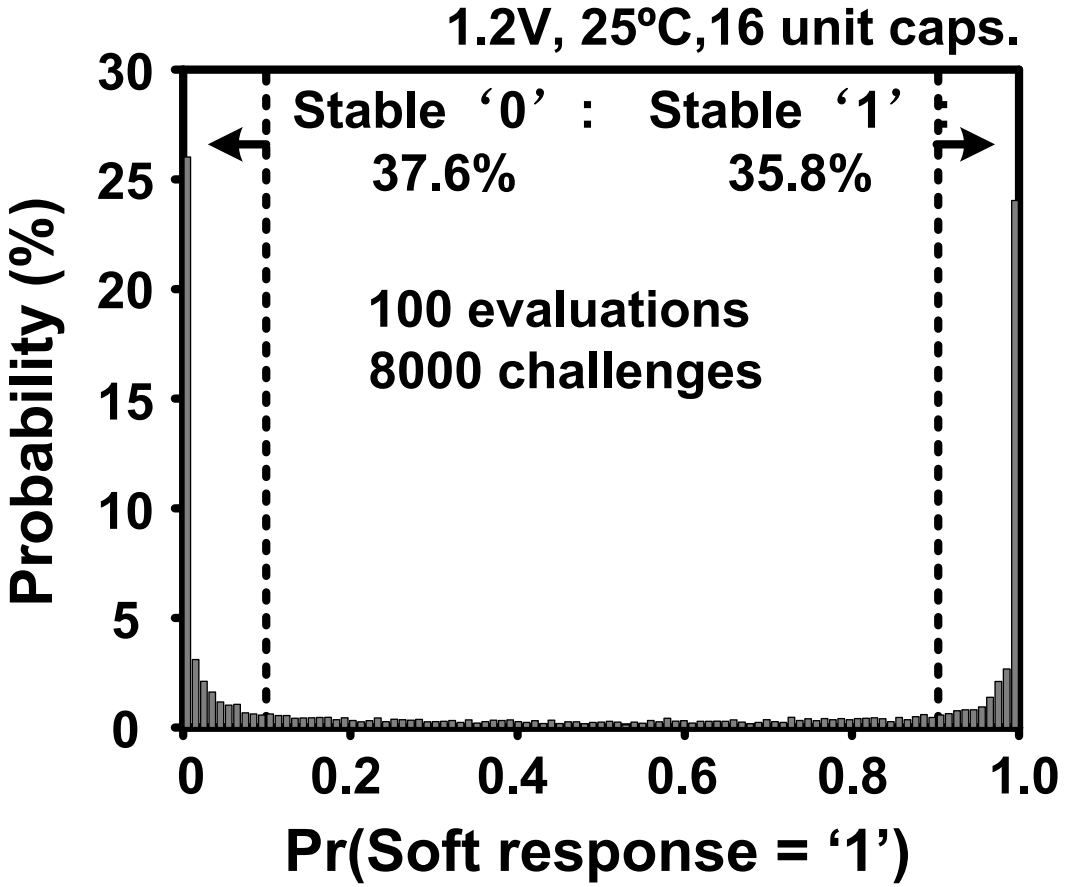


- Soft-response measurement
  - Repetitively evaluating the PUF using the same challenge
  - Counting the number of times the comparator output evaluates to '1' using an on-chip counter

Outline

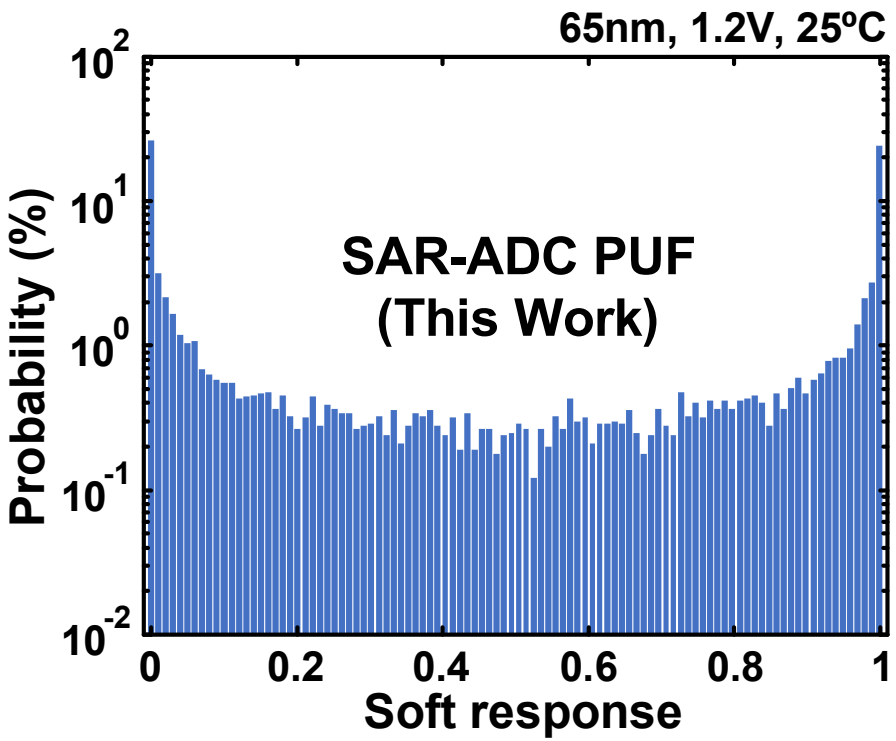
- Background and Motivation
- Proposed SAR-ADC PUF
- 65nm PUF Chip Data
- Summary

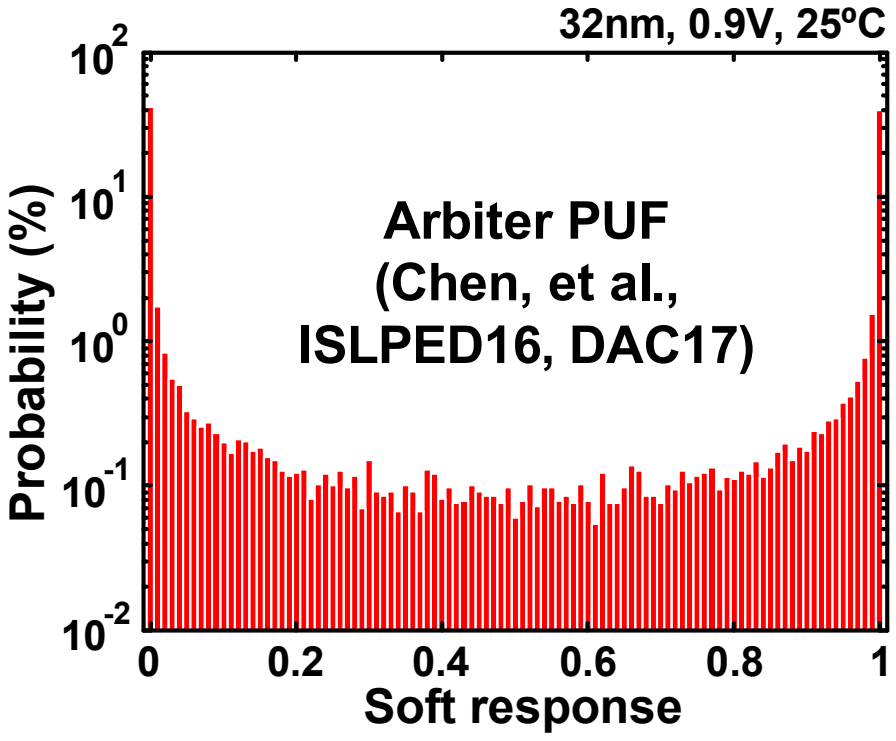
Measured Soft Response



- 8,000 different challenges were applied and each challenge was evaluated 100 times

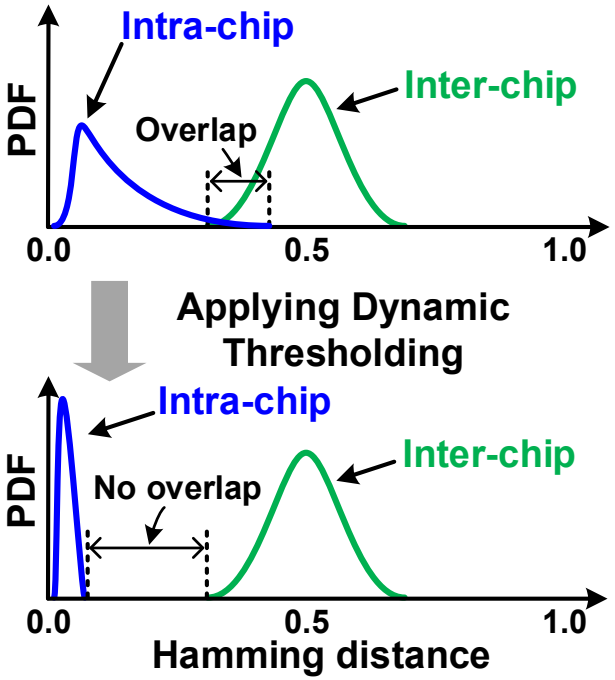
Stability Comparison

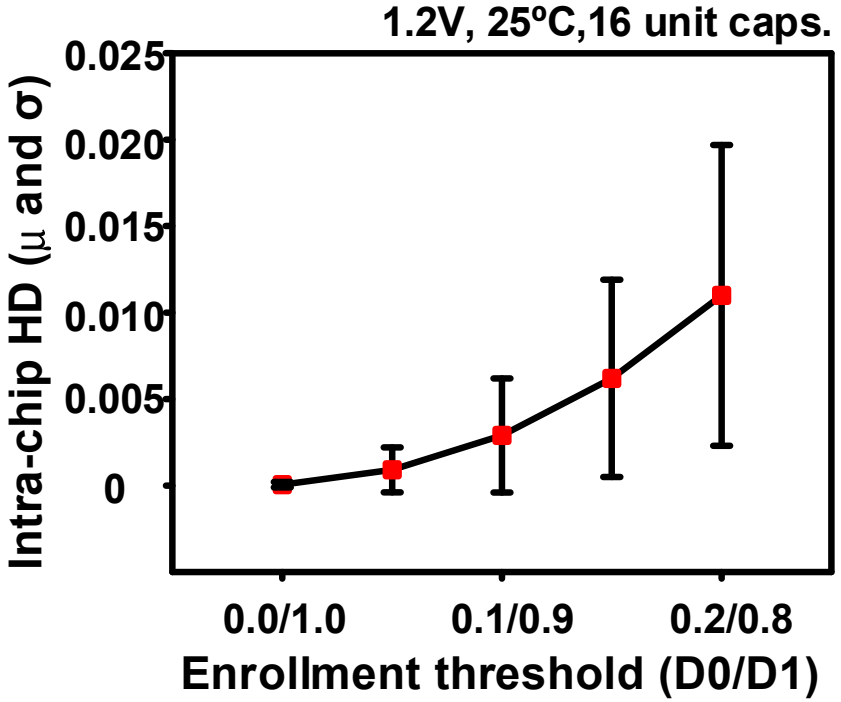




- Stability of SAR-ADC PUF not better than that of Arbiter PUF
- Noise due to active devices in SAR-ADC PUF makes response unstable

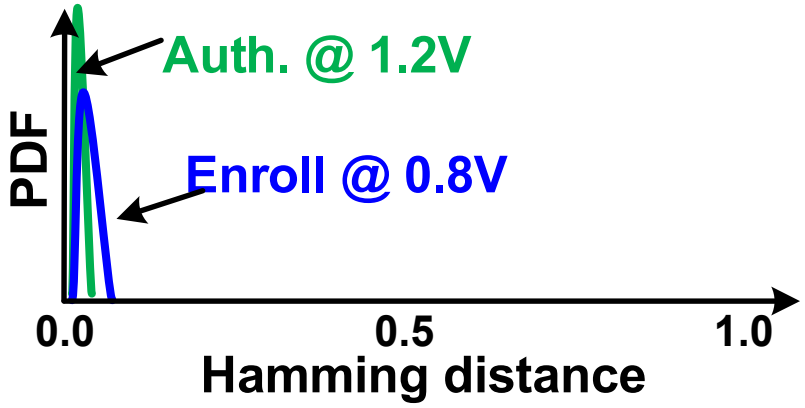
Solution #1: Dynamic Thresholding

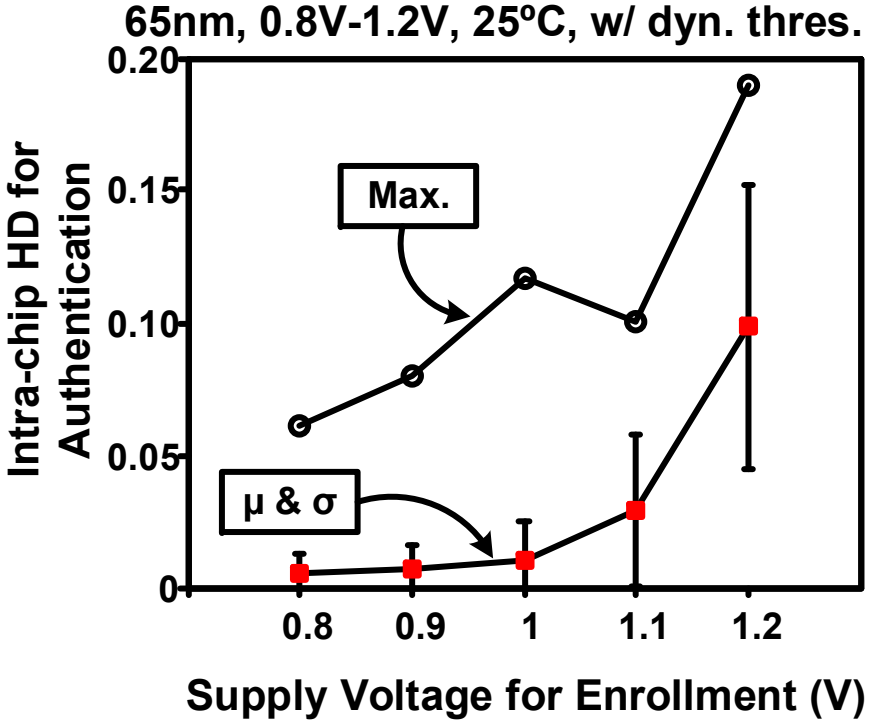




- Improve the consistency and uniqueness by suppressing intra-chip HD
- Approach: Stringent threshold for enrollment, relaxed threshold for authentication

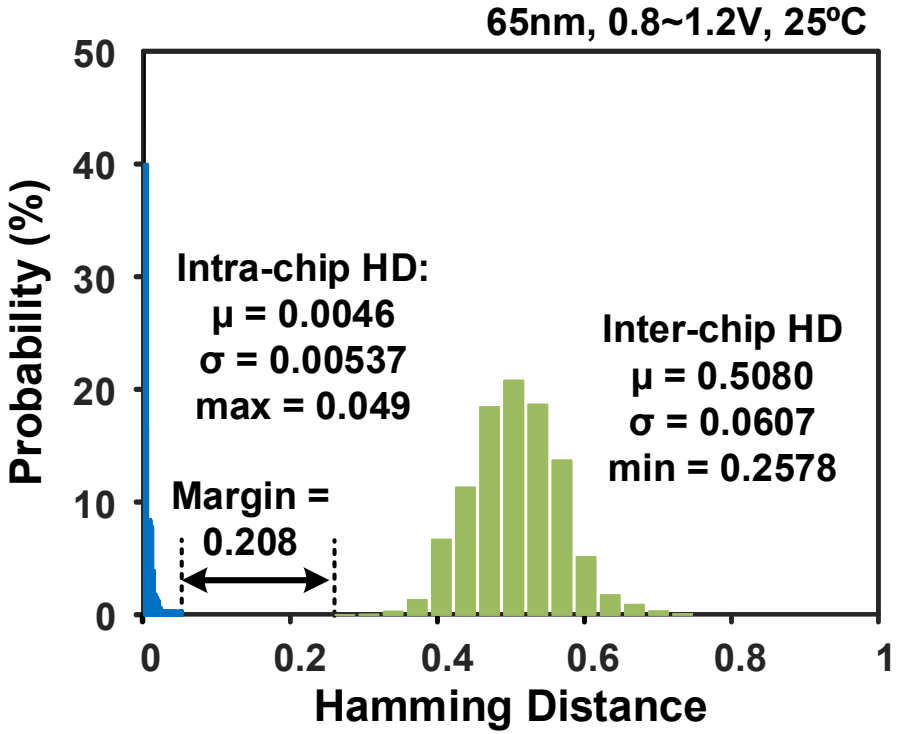
Solution #2: Low VDD Enrollment





- ΔV of SAR-ADC PUF is proportional to VDD → response will be more stable at higher VDDs
- Approach: Low VDD (0.8V) for enrollment, any VDD (0.8-1.2V) for authentication

After Incorporating Solutions #1 and #2



	Intra-chip	Inter-chip
Threshold	Pr('1')<0.1 or Pr('1')>0.9	
# of challenges	8k	80k
Discarded responses	47.8%	
Enrollment VDD Authentication VDD	0.8V 0.8~1.2V	
# of cycles for eval.	990×10	10
# chips	1	10

- 40,000 stable challenges are applied to the 10 different chips with a supply voltage ranging from 0.8V to 1.2V
- Group the CRPs into 312 × 128-bit responses for inter-chip HD eval.:
  - μ = 50.6%, close to the ideal 50% inter-chip HD
  - max(intra-chip) – min(inter-chip) = 20.8%, suggests good uniqueness

Outline

- Background and Motivation
- Proposed SAR-ADC PUF
- 65nm PUF Chip Data
- Summary

Summary

- Capacitance mismatch in a standard SAR-ADC utilized for PUF operation
- 65nm test chip shows worse stability compared to arbiter PUFs due to active devices
- Solutions for overcoming stability issues: Soft response thresholding, low VDD enrollment
- Possible future work: Security analysis of passive device based PUFs

Acknowledgement: This research was supported by the National Science Foundation under grant number CNS-1441639 and the semiconductor research corporation under contract number 2014-TS-2560.